

CLAIMS

What is claimed is:

- 1 1. A method of controlling access of network management requests directed to one or
2 more network devices that participate in a virtual private network, the method
3 comprising the computer-implemented steps of:
4 receiving a request to carry out a management protocol operation;
5 determining an identifier of a virtual private network in the request;
6 identifying, among a plurality of managed objects, a subset of objects that requests
7 associated with the virtual private network are permitted to access; and
8 providing the request with access to only the subset of objects.
- 1 2. A method as recited in Claim 1, further comprising the steps of providing, at one of
2 the network devices, a mapping of a plurality of identifiers of virtual private networks
3 to corresponding views of subsets of managed objects.
- 1 3. A method as recited in Claim 1, further comprising the steps of providing, at one of
2 the network devices, a mapping of a plurality of identifiers of virtual private networks
3 to corresponding views of subsets of managed objects, in the form of one or more
4 entries in a view-based access control model table that associate SNMPv3
5 securityName values to corresponding MIB Views.
- 1 4. A method as recited in Claim 1, further comprising the steps of providing, at one of
2 the network devices, one or more entries in a view-based access control model table
3 that associate SNMPv3 securityName values to corresponding MIB Views, wherein
4 each of the securityName values is associated with a virtual private network, and
5 wherein the corresponding MIB Views represent access control policies applicable to
6 the associated virtual private networks.

1 5. A method as recited in Claim 1, further comprising the steps of providing, at one of
2 the network devices, a mapping of a plurality of identifiers of virtual private networks
3 to corresponding views of subsets of managed objects, and wherein the steps of
4 identifying a subset of objects and providing the request with access comprise the
5 steps of.

6 determining whether the identifier from the request is in the mapping;

7 when the identifier from the request is in the mapping:

8 identifying a management information base variable referenced in the request;

9 based on one or more views referenced in the mapping, determining whether a

10 protocol operation of the request is allowed for the variable;

11 dispatching information identifying the variable and the protocol operation to

12 a code implementation of the protocol operation only when the

13 protocol operation is allowed for the variable.

1 6. A method as recited in Claim 1, further comprising the steps of providing, at one of
2 the network devices, a mapping of a plurality of identifiers of virtual private networks
3 to corresponding views of subsets of managed objects, in the form of one or more
4 entries in a view-based access control model table that associate security name values
5 to corresponding MIB Views, and wherein the steps of identifying a subset of objects
6 and providing the request with access comprise the steps of.

7 determining whether the identifier from the request is in the view-based access control
8 model table;

9 when the identifier from the request is in the view-based access control model table:

10 identifying a management information base variable referenced in the request;

11 based on one or more MIB Views referenced in the view-based access control

12 model table, determining whether a protocol operation of the request is

13 allowed for the variable;

14 dispatching information identifying the variable and the protocol operation to

15 a code implementation of the protocol operation only when the

16 protocol operation is allowed for the variable.

1 7. A method as recited in Claim 1, further comprising the steps of providing, at one of
2 the network devices, one or more entries in a view-based access control model table
3 that associate SNMPv3 securityName values to corresponding MIB Views, wherein
4 each of the securityName values is associated with a virtual private network, and
5 wherein the corresponding MIB Views represent access control policies applicable to
6 the associated virtual private networks, and wherein the steps of identifying a subset
7 of objects and providing the request with access comprise the steps of
8 determining whether the identifier from the request is in the view-based access control
9 model table;
10 when the identifier from the request is in the view-based access control model table:
11 identifying a management information base variable referenced in the request;
12 based on one or more MIB Views referenced in the view-based access control
13 model table, determining whether a protocol operation of the request is
14 allowed for the variable;
15 dispatching information identifying the variable and the protocol operation to
16 a code implementation of the protocol operation only when the
17 protocol operation is allowed for the variable.

1 8. A method as recited in Claim 1, further comprising the steps of:
2 providing, at a network management station that is communicatively coupled to the
3 network devices, a mapping of a plurality of virtual private network identifiers
4 to SNMPv3 securityNames;
5 providing, at the network management station, an executable process that associates a
6 virtual private network identifier with each SNMP request that is issued by the
7 network management station to the network devices.

1 9. A method of controlling access of network management requests directed to one or
 2 more network devices that participate in a virtual private network, the method
 3 comprising the computer-implemented steps of:
 4 receiving a request to carry out a management protocol operation, wherein the request
 5 contains a virtual private network identifier in a security name value;
 6 extracting the security name value and determining a protocol operation that is
 7 embodied in the request;
 8 using a view-based access control model, matching the security name value to a
 9 management information base view that corresponds to the requested
 10 operation;
 11 processing the requested operation only if access is allowed to managed objects in the
 12 management information base, based on the matching management
 13 information base view.

1 10. A method as recited in Claim 9, further comprising the steps of:
 2 determining whether the request can be satisfied;
 3 extracting the security name value from a context string in the request.

1 11. A method as recited in Claim 10, wherein the matching step further comprises the
 2 steps of:
 3 determining whether the security name is in a view-based access control model table;
 4 rejecting and returning the request when the security name is not found in the view-
 5 based access control model table.

1 12. A method as recited in Claim 10, further comprising the steps of:
 2 determining whether the security name is in a view-based access control model table;
 3 when the security name is found in the view-based access control model table:
 4 identifying a management information base variable referenced in the request;

5 based on one or more views referenced in the view-based access control model
6 table, determining whether the protocol operation is allowed for the
7 variable;
8 dispatching information identifying the variable and the protocol operation to
9 a code implementation of the protocol operation only when the
10 protocol operation is allowed for the variable.

1 13. The method as recited in Claim 10, further comprising the steps of:
2 determining whether the security name is in a view-based access control model table;
3 when the security name is found in the view-based access control model table:
4 identifying a management information base variable referenced in the request;
5 based on one or more views referenced in the view-based access control model
6 table, determining whether the protocol operation is allowed for the
7 variable;
8 dispatching information identifying the variable and the protocol operation to
9 a code implementation of the protocol operation only when the
10 protocol operation is allowed for the variable;
11 using a "find first" function, determining whether a virtual private network
12 identifier is referenced in the request, processing the request using
13 managed information objects in a default view when no virtual private
14 network identifier is referenced in the request, and processing the
15 request using management information objects in a view corresponding
16 to the virtual private network identifier only when a virtual private
17 network identifier is referenced in the request.

1 14. A computer-readable medium carrying one or more sequences of instructions for
2 controlling access of network management requests directed to one or more network
3 devices that participate in a virtual private network, which instructions, when
4 executed by one or more processors, cause the one or more processors to carry out the
5 steps of:
6 receiving a request to carry out a management protocol operation;

7 determining an identifier of a virtual private network in the request;
8 identifying, among a plurality of managed objects, a subset of objects that requests
9 associated with the virtual private network are permitted to access; and
10 providing the request with access to only the subset of objects.

1 15. A computer-readable medium as recited in Claim 14, further comprising instructions
2 which, when executed by the one or more processors, cause the one or more
3 processors to carry out the steps of providing, at one of the network devices, a
4 mapping of a plurality of identifiers of virtual private networks to corresponding
5 views of subsets of managed objects.

1 16. A computer-readable medium as recited in Claim 14, further comprising instructions
2 which, when executed by the one or more processors, cause the one or more
3 processors to carry out the steps of providing, at one of the network devices, a
4 mapping of a plurality of identifiers of virtual private networks to corresponding
5 views of subsets of managed objects, in the form of one or more entries in a view-
6 based access control model table that associate SNMPv3 securityName values to
7 corresponding MIB Views.

1 17. A computer-readable medium as recited in Claim 14, further comprising instructions
2 which, when executed by the one or more processors, cause the one or more
3 processors to carry out the steps of providing, at one of the network devices, one or
4 more entries in a view-based access control model table that associate SNMPv3
5 securityName values to corresponding MIB Views, wherein each of the securityName
6 values is associated with a virtual private network, and wherein the corresponding
7 MIB Views represent access control policies applicable to the associated virtual
8 private networks.

- 1 18. A computer-readable medium as recited in Claim 14, further comprising instructions
2 which, when executed by the one or more processors, cause the one or more
3 processors to carry out the steps of providing, at one of the network devices, a
4 mapping of a plurality of identifiers of virtual private networks to corresponding
5 views of subsets of managed objects, and wherein the steps of identifying a subset of
6 objects and providing the request with access comprise the steps of:
7 determining whether the identifier from the request is in the mapping;
8 when the identifier from the request is in the mapping:
9 identifying a management information base variable referenced in the request;
10 based on one or more views referenced in the mapping, determining whether a
11 protocol operation of the request is allowed for the variable;
12 dispatching information identifying the variable and the protocol operation to
13 a code implementation of the protocol operation only when the
14 protocol operation is allowed for the variable.
- 1 19. An apparatus for controlling access of network management requests directed to one
2 or more network devices that participate in a virtual private network, comprising:
3 means for receiving a request to carry out a management protocol operation;
4 means for determining an identifier of a virtual private network in the request;
5 means for identifying, among a plurality of managed objects, a subset of objects that
6 requests associated with the virtual private network are permitted to access;
7 and
8 means for providing the request with access to only the subset of objects.
- 1 20. An apparatus controlling access of network management requests directed to one or
2 more network devices that participate in a virtual private network, comprising:
3 a network interface that is coupled to the data network for receiving one or more
4 packet flows therefrom;
5 a processor;

6 one or more stored sequences of instructions which, when executed by the processor,
7 cause the processor to carry out the steps of:
8 receiving a request to carry out a management protocol operation;
9 determining an identifier of a virtual private network in the request;
10 identifying, among a plurality of managed objects, a subset of objects that
11 requests associated with the virtual private network are permitted to
12 access; and
13 providing the request with access to only the subset of objects.

50325-0571 (Seq. No. 2207)